A NEW APPROACH FOR JPEG FRAGMENTATION POINT DETECTION USING SEQUENTIAL DIFFERENCE BY SEGMENT (SDbS)

TENGKU NORSUHAILA BINTI T AZMI

A thesis submitted in
fulfillment of the requirement for the award of the
Degree of Master of Information Technology

Faculty of Computer Science and Information Technology
Universiti Tun Hussein Onn Malaysia

AUGUST 2019

In the name of Allah, Most Gracious.

I praise and thank Allah.

I would like to express my sincere gratitude to my supervisor,
Dr. Nurul Azma binti Abdullah
for the continuous support and guide of my research.

I would like to thank my family and my friends
for supporting me to finish this research.

This thesis is dedicated to all of you.

ACKNOWLEDGEMENT

I would like to express my sincere gratitude to my supervisor, Dr. Nurul Azma binti Abdullah for her willingness accepting me as her Master student and for the continuous support of my research. Her guidance helped me in all the time of research and writing of this thesis.

I owe my gratitude to Universiti Tun Hussein Onn Malaysia (UTHM) and I am also greatly indebted to Faculty of Computer Science and Information Technology (FSKTM) and Centre for Graduate Studies (CGS) of Universiti Tun Hussein Onn Malaysia (UTHM) for providing good facilities and inspiring environment for me to complete this study comfortably.

Last but not least, I would like to thank my family and my friends for supporting me to finish this research.

ABSTRACT

Digital Forensic is a computer science application and an investigation means, aimed at the prevention of illegal crimes by tracking and retrieving evidence left by cyber criminals. Image recovery is one of the techniques to obtain digital evidences. This technique works by recovering damaged or corrupted digital evidences either through traditional data recovery or file craving. The file craving technique for the most part is to overcome the inherent weaknesses in the traditional data recovery even without any information about the file system. There are many files that can be recovered; images are the most commonly restored files. However, in some cases, JPEG images may be fragmented when stored in the hard disk and it makes it difficult to repair them due to the complexity of determining the fragmentation points. In this research, a technique called Sequential Difference by Segment (SDbS) has been proposed to overcome weaknesses regarding fragmentation detection point of fragmented JPEG images. This technique methodology consists of three steps namely the acquisition of datasets, image segmentation and fragmentation detection. The findings from the third step are the main contributions in this research through the discovery of approaches to detect the fragmentation points using deletion quaternary search and Euclidean Distance to compare pixel values. SDbS has been tested using standard datasets, DFRWS 2006 and DFRWS 2007. They have also been validated using three parameters; average time taken, total image correctly recovered and accuracy of detecting fragmentation point. Based on the results obtained, SDbS has a 19.65% more accurate than SoD, and 0.35% faster than binary search. In other words, SDbS is such a good alternative in addressing problems in detecting the fragmentation points for fragmented JPEG images, compared to SoD and binary search.

ABSTRAK

Forensik Digital adalah aplikasi sains komputer dan sebuah dasar penyiasatan bertujuan pencegahan jenayah haram dengan menjejaki dan mengambil bukti yang ditinggalkan oleh penjenayah siber. Pemulihan imej adalah salah satu teknik untuk mendapatkan bukti digital. Teknik ini berfungsi dengan cara memulihkan bukti digital yang rosak samada melalui pemulihan data tradisional atau ukiran fail. Teknik ukiran fail diperkenalkan untuk mengatasi kelemahan pemulihan data tradisional tanpa perlu mengetahui sistem fail. Forensik digital berupaya memulihkan banyak fail; imej adalah fail yang paling umum dipulihkan. Walau bagaimanapun, dalam beberapa kes, imej-imej JPEG mungkin mengalami kerosakan atau pemecahan (fragmentasi) apabila disimpan dalam cakera keras dan hal ini menyukarkan proses membaik pulih mereka disebabkan oleh kerumitan menentukan titik pemecahan. Dalam penyelidikan ini, teknik Perbezaan Sequential oleh Segment (SDbS) dicadangkan untuk mengatasi kelemahan berkaitan pengesanan pemecahan terhadap imej JPEG yang rosak. Metodologi teknik ini terdiri daripada tiga langkah iaitu pemerolehan dataset, segmentasi imej dan pengesanan pemecahan. Dapatan daripada langkah ketiga merupakan sumbangan utama dalam penyelidikan ini dengan mengemukakan pendekatan untuk mengesan titik pemecahan menggunakan penghapusan oleh carian kuaternary dan Jarak Euclidean untuk membandingkan nilai piksel imej. SDbS telah diuji menggunakan dataset standard, iaitu DFRWS 2006 dan DFRWS 2007. Mereka juga telah disahkan menggunakan tiga parameter iaitu purata masa yang diambil, jumlah imej yang berjaya dibaikpulih dan tahap ketepatan mengesan titik pemecahan. Berdasarkan dapatan kajian, SDbS mempunyai ketepatan 19.65% lebih tinggi berbanding SoD, dan 0.35% lebih cepat daripada carian binari. Dalam erti kata lain, SDbS adalah alternatif yang baik untuk menangani masalah dalam mengesan titik pemecahan bagi imej JPEG yang rosak berbanding SoD dan carian binari.

TABLE OF CONTENTS

DECLARATION	**ii**
DEDICATION	**iii**
ACKNOWLEDGEMENT	**iv**
ABSTRACT	**v**
ABSTRAK	**vi**
TABLE OF CONTENTS	**vii**
LIST OF TABLES	**xi**
LIST OF FIGURES	**xiii**
LIST OF SYMBOLS AND ABBREVIATIONS	**xiv**
LIST OF APPENDICES	**xvi**
LIST OF PUBLICATIONS	**xvii**

CHAPTER 1	**INTRODUCTION**		**1**
	1.1	Background of Study	1
	1.2	Research Motivation	2
	1.3	Research Objectives	6
	1.4	Scope of Study	7
	1.5	Organization of Thesis	7
CHAPTER 2	**LITERATURE REVIEW**		**8**
	2.1	Introduction	8
	2.2	Image	9
		2.2.1 Overview of JPEG Image	9
		2.2.2 Overview of BMP Image	10
		2.2.3 Comparison between JPEG and BMP image	14
	2.3	File Structure	16
		2.3.1 Non-fragmented files	16
		2.3.2 Fragmented Files	17
	2.4	Dataset used for file carving	18
	2.5	Non-fragmented and fragmented carving techniques	19
		2.5.1 Carving non-fragmented files	19
		2.5.2 Carving fragmented files	20
	2.6	Fragmentation Point Detection	21
		2.6.1 Linear searching	21
		2.6.2 Binary searching	22
		2.6.3 Sum of Difference	23
		2.6.4 Euclidean Distance	24
		2.6.5 Fragmentation Point Detection Handling	25
		2.6.5.1 Image Fragment Carving Algorithms based on Pixel Similarity	26
		2.6.5.2 Fragmentation Point Using Unique Hex Patterns (UHP)	27
		2.6.5.3 Image fragment identification	

using machine learning 27
2.6.5.4 Sum of Differences (SoD) of boundary pixels of two fragments 28
2.6.5.5 Comparative analysis of existing fragmentation detection techniques 29
2.7 Performance Metrics for Detecting Fragmented Image 31
2.7.1 Average Time Taken 31
2.7.2 Accuracy Rate 32
2.8 Chapter Summary 32

CHAPTER 3 RESEARCH METHODOLOGY 34
3.1 Introduction 34
3.2 Research Process 34
3.3 Framework of SDbS 36
3.3.1 Dataset Acquisition 37
3.3.2 Fragmentation Point Detection 38
3.3.3 Image Segmentation 40
3.3.4 Getting Euclidean Distance value 42
3.4 Chapter Summary 43

CHAPTER 4 IMPLEMENTATION 44
4.1 Introduction 44
4.2 Datasets Acquisition 44
4.3 Segmentation of image 50
4.4 Obtaining Euclidean Distance value 52
4.5 Chapter Summary 53

CHAPTER 5 RESULTS AND DISCUSSION 54
5.1 Introduction 54
5.2 Detecting fragmentation point 54
5.3 Comparison with other tools and techniques 54

		5.3.1 Validation Measurement: Total image recovered	55
		5.3.2 Validation Measurement: Percentage accuracy	57
		5.3.3 Validation Measurement: Average Time Taken	59
	5.4	Comparison Results	60
	5.5	Chapter Summary	62
CHAPTER 6	**CONCLUSIONS AND RECOMMENDATIONS**		63
	6.1	Contributions of the study	63
		6.1.1 Objective 1	64
		6.1.2 Objective 2	64
		6.1.3 Objective 3	64
	6.3	Limitation of Research Work	65
	6.4	Recommendations for Future Work	65
	REFERENCES		**67**
	APPENDIX		**70**
	VITAE		**71**

LIST OF TABLES

1.1	Research terminologies	3
2.1	JPEG file marker	10
2.2	BMP file structure	11
2.3	Description of *BMP Header*	12
2.4	Description of *BMP InfoHeader*	13
2.5	Comparison of JPEG and BMP image formats	14
2.6	Different of fragmented JPEG and BMP image	15
2.7	Definition of term	18
2.8	Datasets file	19
2.9	Fragmentation Detection Comparative Analysis	30
3.1	Illustration of JPEG image scenarios	38
3.2	Differences between existing model and SDbS model	39
3.3	Binary search and proposed quaternary search	41
3.4	SoD and ED values	42
4.1	The output files from the carving process for DFRWS 2006 dataset.	45
4.2	The output files from the carving process for DFRWS 2007 dataset.	48
4.3	Image Segmentation using SDbS	50
4.4	Pixel value of each segment	51
4.5	ED value of each segment	52
4.6	ED value of each segment	53
5.1	Comparison of SOD and SDbS (ED) based on total image recovered (DFRWS 2006)	54
5.2	Comparison of SOD and SDbS(ED) based on total image recovered (DFRWS 2007)	54

5.3	Accuracy of detecting fragmentation point DFRWS 2006	56
5.4	Accuracy of detecting fragmentation point DFRWS 2007	56
5.5	Average time taken DFRWS 2006	57
5.6	Average time taken DFRWS 2007	58
5.7	Summary DFRWS 2006 dataset	59
5.8	Summary DFRWS 2007 dataset	59

LIST OF FIGURES

1.1	First fragment of JPEG file	5
1.2	Second fragment of JPEG file	6
2.1	BMP Header open in Hex Editor	12
2.2	BMP Data structure	13
2.3	Non-fragmented files	16
2.4	Fragmented files	17
2.5	Fragmentation point in a fragmented file	22
2.6	Comparing pixel values by pixel similarity	26
2.7	Workflow of SoD technique	29
3.1	Research Process	35
3.2	Framework of SDbS	36
3.3	A magnified view of fragmentation point	39
3.4	Segmentation of fragmented image	40

LIST OF SYMBOLS AND ABBREVIATIONS

x_i	-	RGB value of the pixel from one fragment
y_i	-	RGB value of the corresponding pixel from the other fragment
BGC	-	Bifragment Gap Carving
BMP	-	Bitmap
DF	-	Digital Forensics
DFRWS	-	Digital Forensic Research Workshop
DHT	-	Define Huffman Table
DIB	-	Device Independent Bitmap
DQT	-	Define Quantization Table
ED		Euclidean Distance
EOF	-	End of File
EOI	-	End of Image
FP	-	Fragmentation Point
GIF	-	Graphic Interchange Format
HTML	-	Hypertext Markup Language
JEIDA	-	Japan Electronic Industry Development Association
JPEG	-	Joint Photographic Expert Group
MB	-	MegaByte
n	-	number of pixel pairs involved in the boundaries
PDF	-	Portable Document Format
PNG	-	Portable Network Graphics
RGB	-	Red Green Blue
SDbS	-	Sequential Difference by Segment
SoD	-	Sum of Differences
SOF	-	Start of File

SOI	-	Start of Image
SOS	-	Start of Scan
UHP	-	Unique Hex Patterns
ZIP	-	Zone Information Protocol

LIST OF APPENDICES

APPENDIX	TITLE	PAGE
A	Table A.1: Gantt chart of research activities	70

LIST OF PUBLICATIONS

Proceedings:

Tengku Norsuhaila T Azmi, Nurul Azma Abdullah, Nurul Hidayah Ab Rahman, Isredza Rahmi A. Hamid, Chuah Chai Wen. (2017). Image Size Variation Influence on Corrupted and Non-viewable BMP Image. In *Proceedings of the International Conference on Advances in Computing and Intelligent System* (ICACIS 2017), 6 May 2017, Melaka, Malaysia.

CHAPTER 1

INTRODUCTION

1.1 Background of Study

Nowadays, the use of Internet has been tremendously increased by the way technology development and Information Technology change how people live, work, play, and learn (Ramey, 2012). However, there are many issues regarding the use of Internet such as phishing, sabotage and cybercrime activities which are hard to be brought to justice. Therefore, with the introduction of Digital Forensics (DF) which has been used as a platform to recover and analyse of material found in digital devices, this has make it possible to bring perpetrators of cybercrimes to justice (Garfinkel, 2010). DF can be defined as the application of computer science and investigative policy for illegal crime purposes involving the evaluation of digital evidence after proper search authority, chain of custody, validation with mathematics, use of validated tools, repeatability, reporting, and possible skilled presentation (Wang, 2007). It is used to retrieve the digital evidence left by a cyber perpetrator. Recovering files from digital media is an important skill in a process of prosecuting the perpetrator (Bhadran & Povar, 2011). Traditional data recovery and file carving are two ways of recovering digital evidences in digital storage.

Traditional data recovery relies on file system structures to recover data that has been deleted where the file allocation table or metadata exists. In a case where the file allocation table or metadata is damaged, file carving is used to overcome the

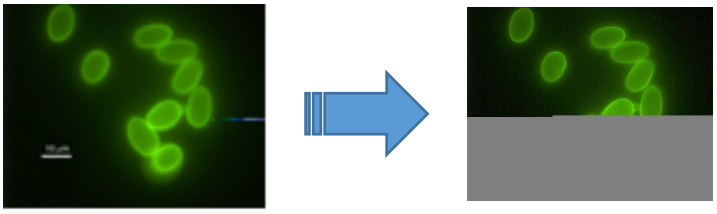
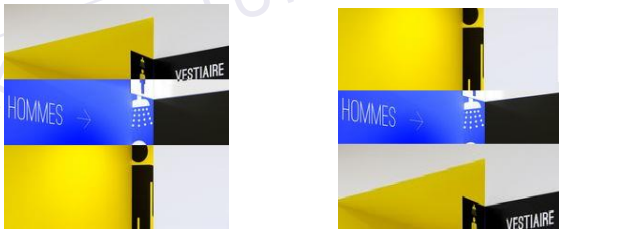
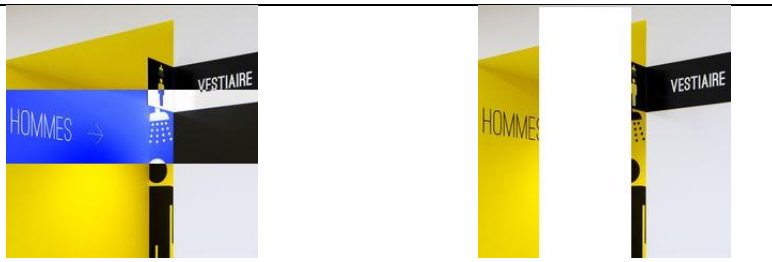
limitation of traditional data recovery. Simply put, file carving is a process of recovering files from a disk without knowing the file system (Veenman, 2007). There are many files that can be recovered from the target disk but images are the most common file type used by forensic analyst that help in investigating cases related to cybercrimes. There are many formats of image such as JPEG, bitmap, GIF and PNG, but JPEG is the most popular format used on the Internet because JPEG files are easy to compress and very lossy that can advance in Internet transferring processes (Attimarad & Viraktamath, 2011).

1.2 Research Motivation

A file can be fragmented or divided into two fragments or more that require an additional technique to be recovered. Fragmentation can be introduced when same or different file formats are embedded in a file. JPEG files can be fragmented by the existence of other kinds of files such as Word, PDF and Excel before the end of JPEG file. Fragmentation using the same format happens when a JPEG file is fragmented by another JPEG file.

Table 1.1 shows the terminologies of research, conducted in this research. Types of digital evidence used, types of fragmented file and how fragmentation occurred were shown in the table below.

Table 1.1: Research terminologies

Terminology	Image
Fragmentation	 Complete file — Fragmented file
Single vs. Multiple fragmentation point	 Single fragmentation point — Multiple fragmentation point
Linear vs. Non-linear fragmentation	 Linear fragmentation — Non-linear fragmentation
Fragmentation- Vertical vs. horizontal	 Horizontal – possible in fragmentation — Vertical – not possible in fragmentation

Based on Table 1.1, an image is a type of digital evidence that can be recovered. In this research, JPEG format was used because JPEG has been the most popular format used on the Internet. Through file carving, JPEG image can be recovered easily if file is completed and can be viewed. However, in some inconvenience, JPEG images are hard to recover when they are fragmented, for instance, because they are not stored in contiguous order in storage. Fragmented JPEG images are difficult to recover due to the complexities of determining fragmentation point. Fragmentation point can be determined when a file is fragmented.

In this research, focussing on fragmented not corrupted image which is fragmentation occurs when files are not stored in the contiguous clusters on disk and separated by unknown clusters in between while corruption occurs when errors in computer data that occur during writing, reading, storage, transmission, or processing, which introduce unintended changes to the original data that might not be opened or might open with some of the data corrupted. There are two types of fragmentation for JPEG images that have been studied in this research – single and multiple fragmentation points. Single fragmentation point refers to a condition in which a JPEG file is fragmented into two parts, and fragmented with another JPEG image while multiple fragmentation point refers to a situation in which two JPEG files are fragmented into multiple parts, and fragmented with another JPEG image as illustrated in Table 1.1.

Fragmentation can also be linear and non-linear. Linear fragmentation occurs when file present in adjacent order while non-linear occurs when files are not in contiguous order as in original file. In a disk, files are stored by writing the data from left to right of the disk. Hence, when a file is fragmented, there is a high possibility for it to fragment horizontally, but not vertically.

In terms of detecting fragmentation point techniques, there are only some of techniques available today. One of techniques, according to Al-Badi (2013), is by assuming that all fragmentation points were detected correctly before fragments can be identified. In this case, there will be inability to detect fragmentation point of image correctly because researcher was just assuming a location of fragmentation point. This research attempted to study a better way to detect single and multiple fragmentation points of image correctly. Mohamad et al. (2010) proposed myKarve

as a tool to carve contiguous and linearly fragmented images, caused by other file formats. However, it only focussed on JPEG files which were fragmented with other types of files such as Word, PDF and Excel. Hence, this research attempted to study a way of detecting fragmentation point with the same file format in one file. Another technique used by Kumar (2016) was cluster by cluster analysis to detect fragmentation point. Moreover, Abdullah (2013) introduced a technique called deletion by binary search to detect fragmentation point which has been used to separate a file into several individual fragments. It may take more processing times to detect fragmentation points. Consequently, this research attempted to study a way to reduce times taken to detect fragmentation point in images.

There are two considerations for fragmentation between JPEG files. The first scenario is when a fragmented JPEG file is fragmented with another image as shown in Figure 1.1. Let say they are two JPEG files called F1 and F2. The second scenario is when fragmented JPEG file is fragmented with two or more parts of other image files. In Figure 1.1, F1 is fragmented in which it splits into two parts. This file is fragmented with another JPEG image, F2. This condition is called single fragmentation JPEG files.

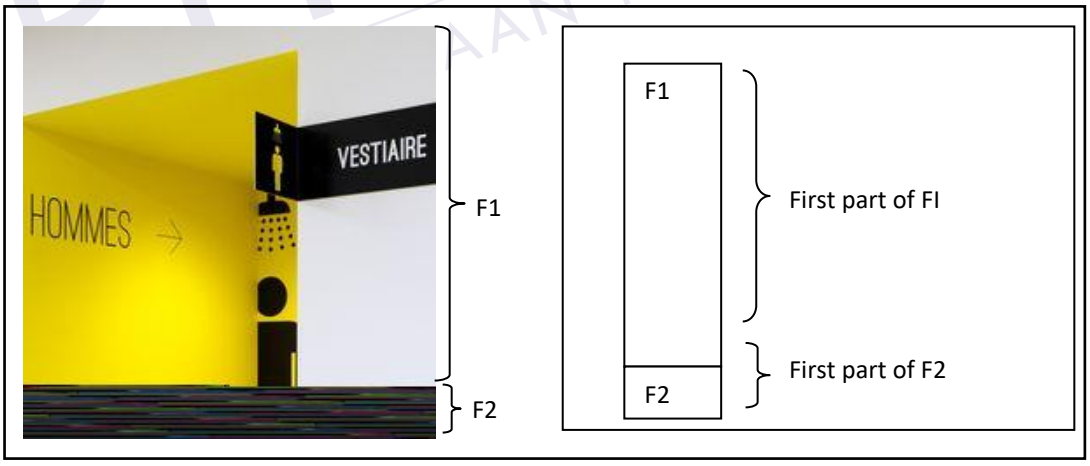


Figure 1.1: First fragment of JPEG file

In the second scenario, JPEG file are fragmented into two or more parts with other images. Figure 1.2 shows two JPEG files in which the second part of F1 is

separated by another image, F2. In both scenarios, it is important to identify the boundary of each file to differentiate between those two files. This file is fragmented with other two or more parts of JPEG image, F2. This condition is called multiple fragmentation JPEG files.

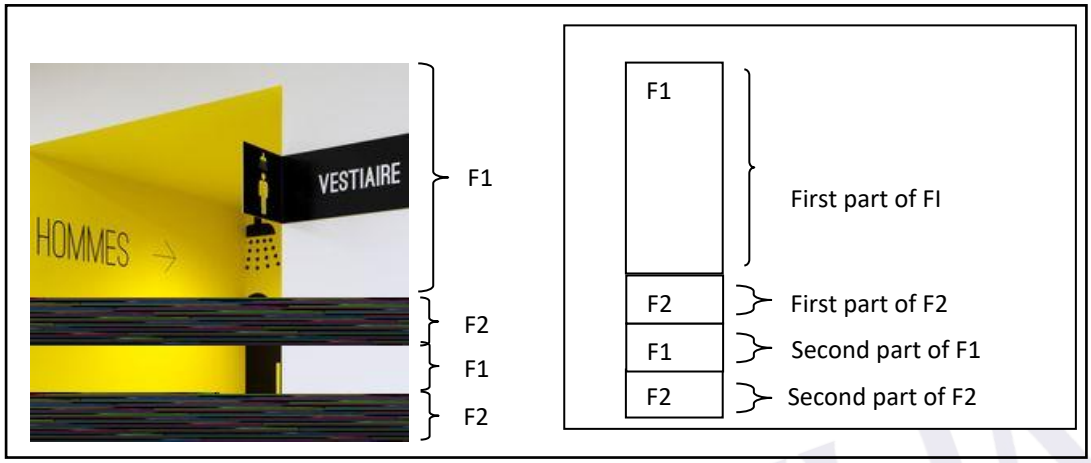


Figure 1.2: Second fragment of JPEG file

Fragmentation with the same file format is harder to handle compared with fragmented images caused by other formats because the headers are similar and indistinguishable. To handle these limitations, this research has been focussing on BMP format to detect fragmentation point for the fragmented JPEG files. BMP image are preferrable in image processing compared to another formats because they contain all the image information in a simple format. Therefore, in order to investigate the fragmentation point in JPEG, the file is required to be converted into BMP format.

1.3 Research Objectives

The objectives of this research were:

1. To propose an approach; Sequential Difference by Segment (SDbS) for detecting fragmentation point of JPEG images.
2. To implement SDbS approach.

3. To evaluate and compare the performance of SDbS approach with Sum of Difference and binary searching technique according to average time taken, total correctly recovered image and accuracy of detecting fragmentation point of fragmented JPEG images.

1.4 Scope of Study

This research focused on comparing pixel value technique for detecting fragmentation point of JPEG images including linear and non-linear fragmentation situations where JPEG files were fragmented with missing fragments. Therefore, only RGB coloured JPEG image will be used in this research because of the need to compare pixel values of image. Not only that, this study also focused on two types of fragmentation for JPEG images – single and multiple fragmentations. The performance metrics were evaluated in this research to improve the accuracy on detecting fragmented JPEG images and reducing time taken to detect fragmentation point.

1.5 Organization of Thesis

The rest of the chapters were organized as follows: Chapter 2 discussed a general Digital Forensics field, - JPEG and BMP file format, the traditional data recovery and file carving, techniques used to determine fragmentation point, file fragmentation, existing carving techniques and performance metrics that were used in relation to this research. Chapter 3 discussed the research framework and algorithms. Chapter 4 discussed the processes of SDbS implementation and detecting fragmentation handling. Chapter 5 discussed the results of detecting fragmentation point of JPEG images and comparison between other techniques. Chapter 6 concluded the research and provided suggestions for future work.

CHAPTER 2

LITERATURE REVIEW

2.1 Introduction

Nowadays, there have been increasing numbers of crime involving computers and multimedia files and it is not uncommon for suspects to delete, damage or modify the files before they get caught or data are seized by the law enforcement officer (Garfinkel, 2007). Child phonography is one of the problems in criminal investigation. Due to this, the police need a better mechanism to scan hard disks and networks for possible illegal material more effectively (Wortley & Smallbone, 2010). Digital Forensics can be used in criminal investigations, civil litigation, intelligence, and administrative matters. Reassembling the photos from deleted file fragments becomes an important technique to recover the digital evidence in these cases.

This chapter discussed the Digital Forensics, file carving, JPEG and Bitmap image, fragmentation, and technique to detect fragmentation image. There are many ways to define and explain Digital Forensics but generally it can be defined as the application of computer science and investigative strategies for a criminal crime purposes involving the evaluation of digital evidence after proper search authority, chain of custody, validation with mathematics, the use of validated tools, repeatability, reporting, and possible expert presentation (Zatyko, 2007). During Digital Forensics investigation, image carving is one of the digital evidence acquiring techniques. Carving is widely used for forensics and data recovery that can recover files from a device that has been damaged and has their directory entries reallocated to other files. Recovering the image files from damaged devices is an important technique to recover the digital evidence in these issues.

REFERENCES

Abdullah, N. A. (2013). Carving Linearly JPEG Images Using Unique Hex Patterns (UHP). *Advanced Data and Information Engineering*, pp. 291-295.

Attimarad, G. V. and Viraktamath, S. V. (2011). Impact of Quantization Matrix on the Performance of JPEG. International Journal of Future Generation Communication and Networking, 4 (3), pp. 107-118.

Bhadran, V. K. and Povar, D. (2011). Forensics Data Carving. Digital Forensics and Cyber Crime, 53, pp. 137-148.

Caroline (2010). The 5 Types of Digital Image Files. Retrieved on May 14, 2010, from http://www.ivanexpert.com/blog/2010/05/the-5-types-of-digital-imagefiles-tiff-jpeg-gif-png-and-raw-image-files-and-when-to-use-each-one/

Chai, I. & White, J. D. (2006). Structuring Data and Building Algorithms: An ANSI Based Approach. Singapore: McGraw Hill.

Cohen, M. (2007). Advanced Carving Techniques. *Digital Investigation, 4(1-4)*, 119-128.

Garfinkel, S. (2007). Carving Contiguous and Fragmented Files with Fast Object Validation. *Journal of Digital Investigation*, 2-12.

Garfinkel, S. L. (2010). Digital Forensics Research: The Next 10 Years. Digital Investigation, 7(1), pp. S64-S73.

Grenier, C. (2011, October). *Data carving log.* Retrieved from http://www.cgsecurity.org/wiki/PhotoRec

Isner, J.D. (2003). Computer Forensics: An emerging practice in the battle against cybercrime. Retrieved on December 22, 2010, from SANS Institute: http://www.giac.org/certified_professionals/practicals/gsec/2797.php

Jupiter (2013). Comparison of BMP, JPG, GIF and PNG formats. Retrieved on January 27, 2013, from http://techstumbling.com/comparison-of-bmp-jpg-gifand-png-formats/

Kloet, S. J. (2007). *Measuring and Improving the Quality of File Carving Methods.* Eindhoven University of Technology.

Li, B. W. (2012). Image Fragment Carving Algorithms based on Pixel Similarity. *Fourth International Conference on Multimedia Information Networking and Security*, pp. 979-982.

Li, Q., Sahin, B., Chang, E. C. and Thing, V. L. L. (2011). Proceeding of the International Conference on Multimedia Computing and Systems. pp. 1-6.

Mathew, A. (2016). A Method for Carving Fragmented Document and Image Files. *International Conference on Advances in Human Machine Interaction (HMI - 2016)*, 978.

Matthews, R. (2012). Digital Image File Types Explained. Retrieved on 2012, From http://users.wfu.edu/matthews/misc/graphics/formats/formats.html

Memon, N. a. (2006). Automated reassembly of the file fragmented images using greedy algorithms. *Journal IEEE Trans. Image Processing*, 15(2), pp. 385-393.

Mohamad, K. M. (2009). Single-byte-marker for detecting JPEG JFIF header using FORIMAGE-JPEG. *Proceeding of NCM 2009*, 1693-1698.

Mohamad, K. M., Patel, A., Herawan, T., Mat Deris, M. (2010). myKarve: Jpeg image and thumbnail carver. Journal of Digital Forensic Practice. 3, pp.74-97.

Pal, A., Sencar, H.T. and Memon, N. (2008). Detecting File Fragmentation Point Using Sequential Hypothesis Testing. *Digital Investigation, 5*, pp. S2-S13.

Pal, A. and Memon, N. (2009). The evolution of file carving. *IEEE Signal Processing Magazine*, 26(2). pp. 59-71. Retrieved October, 2011, from http://digital-assembly.com/technology/research/pubs/ieee-spm-2009.pdf.

Park, J. H. (2012). *International Journal of Information and Communication Technology*, 1-3.

Ramey. K. (2012). Technological Advancements and Their Effects on Humanity. Retrieved on November 12, 2012, from http://www.useoftechnology.com/technological-advancements-effects-humanity/

Sportiello, L. a. (2012). Context-Based File Block Classification. in G. Peterson, and S. Shenoi (Eds.). *Advances in Digital Forensics VIII, Springer Berlin Heidelberg.*, pp. 67-82.

Uzun, E. & Sencar, H. T. (2015). Carving Orphaned JPEG File Fragments. *IEEE Transactions On Information Forensics and Security. 10(8)*, pp. 1549-1563.

Veenman, C. J. (2007). Statistical Disk Cluster Classification for File Carving. *The Third International Symposium on Information Assurance and Security. Manchester.*, 393-398.

Viraktamath, S. V. and Attimarad, G. V. (2011). Impact of Quantization Matrix on the Performance of JPEG. *International Journal of Future Generation Communication and Networking, 4 (3),* pp. 107-118.

Wang, S. (2007). Measures of Retaining Digital Evidence to Prosecute Computer Based Cybercrimes. Computer Standards & Interfaces, 29(2), pp.216-223

Wortley, R. & Smallbone, S. (2010). *Child Pornography on the Internet.* Retrieved on December 22, 2010, from US Department of Justice: http://www.cops.usdoj.gov/files/ric/Publications/e04062000.pdf

Zatyko, K. (2007, February 01). *Defining Digital Forensics.* Retrieved from http://www.forensicmag.com/article/2007/01/commentary-defining-digital-forensics